ELSEVIER

Discrete Mathematics 176 (1997) 285–298

DISCRETE MATHEMATICS

Corrigendum*

On Ádám's conjecture for circulant graphs

Mikhail Muzychuk[1]

Department of Mathematics and Computer Science, Bar-Ilan University, 52900 Ramat-Gan, Israel

Received 7 July 1995; revised 22 March 1996

Abstract

Ádám's (1967) conjecture formulates necessary and sufficient conditions for cyclic (circulant) graphs to be isomorphic. It is known that the conjecture fails if n is divisible by either 8 or by an odd square. On the other hand, it was shown in [7] that the conjecture is true for circulant graphs with square-free number of vertices. In this paper we prove that Ádám's conjecture remains also true if the number of vertices of a graph is twice squarefree.

1. Introduction

A *cyclic* (*circulant*) graph is one that admits the regular cyclic group as a group of automorphisms. Ádám [1] was the first who considered the necessary and sufficient conditions for cyclic graphs to be isomorphic. He conjectured that, if two cyclic graphs are isomorphic, then the isomorphism between them may be realized by an automorphism of the corresponding cyclic group.

It was shown that Ádám's conjecture is false if n is divisible by either 8 or by an odd square (see, e.g., [3,4]). Pálfy supposed that the conjecture remains true if n is a square-free or twice square-free number (history of the topic is considered in [9,7]).

Recently, it was shown in [7] that the conjecture is valid if the number of graph vertices is not divisible by a square. In this paper we show that Ádám's conjecture also holds for twice square-free numbers.

The idea of the proof is similar to the proof given in [7] for a square-free case. Nevertheless, to make the paper self-contained we repeat in Section 2 and 3.1 the basic definitions and some results from [7].

The proof of the main result is contained in Section 3.

* Unfortunately, due to a technical error, a wrong version of this paper was published in Discrete Mathematics 167/168 (1997) 497–510.

[1] Partially supported by the Ministry of Science of Israel and by German-Israeli Foundation for Scientific Research and Development.

PII S0012-365X(96)00214-8

2. Basics

2.1. Circulant graphs

Let C_n be the cyclic group of order n with unit element 1, where the group operation is written multiplicatively. The directed *circulant* (*cyclic*) graph $\Gamma_n(B)$ determined by $B \subseteq C_n$ has vertex set C_n, and edges $\{(g_1, g_2) \in C_n \times C_n \mid g_1 g_2^{-1} \in B\}$. The undirected circulant graph $\Gamma_n(B)$ is a special case of the directed one if $B = B^{-1}$. Let $S(X)$ denote the symmetric group on a set X. Two circulant graphs $\Gamma_n(B_1)$ and $\Gamma_n(B_2)$ are *isomorphic* if they are isomorphic as usual graphs, i.e., there exists a permutation $\pi \in S(C_n)$ such that $g_1 g_2^{-1} \in B_1 \Leftrightarrow g_1^{\pi}(g_2^{\pi})^{-1} \in B_2$. We shall say that these circulant graphs are *conjugate by multiplier* if there exists a number m relatively prime to n such that $B_2 = \{b^m \mid b \in B_1\}$. It is clear that conjugate graphs are isomorphic. The converse statement is known as *Ádám's conjecture* for circulant graphs. To formulate the main result of this paper we need the following definition. Let us say that $n \in N$ is an *almost square-free* number if it is not divisible by 8 and by an odd square.

Theorem 2.1. *If n is an almost square-free number, then two circulant graphs $\Gamma_n(B_1)$ and $\Gamma_n(B_2)$ are isomorphic if and only if they are conjugate by multiplier.*

The group $\mathrm{Aut}(\Gamma_n(B))$ consisting of all automorphisms of the graph $\Gamma_n(B)$ contains the cyclic subgroup which acts regularly on itself by multiplication. Therefore, the next subsection contains the necessary information about permutation groups with a regular subgroup.

2.2. Permutation groups containing a regular subgroup and Schur rings

Let H be a finite group and K be a field. We denote the group algebra over K as KH. For any $B \subseteq H$ we define $\underline{B}$ as the formal sum $\sum_{a \in B} a \in KH$. Elements of this form will be called *simple quantities* [11].

Consider a permutation group $(G; H)$ containing $(H; H)$ as a regular subgroup acting on itself by right multiplication. Let $1 \in H$ be the unit of H. Denote by $T_0 = \{1\}$, $T_1, \ldots, T_r$ the complete set of orbits of the stabilizer $G_1 = \{g \in G \mid 1^g = 1\}$. The *transitivity module* $V(H, G_1)$ of the group G_1 is the vector space spanned by $\underline{T}_i$, $i = 0, 1, \ldots, r$.

A combinatorial generalization of the properties of transitivity modules yields the notion of *Schur ring* [11].

A subalgebra $\mathscr{A} \subseteq \mathbb{Q}H$ of the group algebra $\mathbb{Q}H$ is called a Schur ring (briefly an *S-ring*) over H if the following conditions are satisfied:

(S1) There exists a basis of $\mathscr{A}$ consisting of simple quantities $\underline{T}_0, \underline{T}_1, \ldots, \underline{T}_r$;

(S2) $T_0 = \{1\}$ and $\bigcup_{i=0}^{r} T_i = H$;

(S3) $T_i \cap T_j = \emptyset$ if $i \neq j$;

(S4) For each $i \in \{0, 1, \ldots, r\}$ there exists an $i' \in \{0, 1, \ldots, r\}$ such that $T_{i'} = \{t^{-1} \mid t \in T_i\}$.

The basis $\underline{T}_0, \ldots, \underline{T}_r$ is called the *standard basis* and the simple quantities $\underline{T}_i$ (resp. the sets T_i) are called *basic quantities* (resp. *basic sets*) of $\mathscr{A}$. The notation $\mathscr{A} = \langle \underline{T}_0, \ldots, \underline{T}_r \rangle$ means that $\underline{T}_0, \ldots, \underline{T}_r$ is the standard basis of $\mathscr{A}$. We say that a set $B \subseteq H$ belongs to $\mathscr{A}$ (and write this as follows $B \in \mathscr{A}$) if $\underline{B} \in \mathscr{A}$. It is clear that an S-ring $\mathscr{A}$ is closed under all set-theoretical operations over the subsets belonging to $\mathscr{A}$. An S-ring $\mathscr{B}$ over the group H is an S-*subring* of an S-ring $\mathscr{A}$ defined over the same group H if $\mathscr{B} \subseteq \mathscr{A}$. The connection between Schur rings and transitivity modules is given by the following statement ([11, Theorem 24.1]):

Theorem 2.2. *The transitivity module $V(H, G_1)$ is an S-ring over H.*

The group $\mathrm{Aut}(\mathscr{A})$ of all automorphisms of an S-ring $\mathscr{A}$ is defined in [6] as the intersection $\mathrm{Aut}(\mathscr{A}) = \mathrm{Aut}(\Gamma_H(T_0)) \cap \cdots \cap \mathrm{Aut}(\Gamma_H(T_r))$, where $\Gamma_H(T_i)$ is the Cayley graph over H whose set of edges is $\{(h_1, h_2) \mid h_1 h_2^{-1} \in T_i\}$. In other words, $\mathrm{Aut}(\mathscr{A})$ consists of all permutations $\pi \in S(H)$ satisfying the condition $h_1 h_2^{-1} \in T_i \Rightarrow h_1^\pi (h_2^\pi)^{-1} \in T_i$ for all $h_1, h_2 \in H$ and $i \in \{0, \ldots, r\}$. If $\mathscr{B} \subseteq \mathscr{A}$ are two S-rings over the same group H, then $\mathrm{Aut}(\mathscr{B}) \geqslant \mathrm{Aut}(\mathscr{A})$.

The group $\mathrm{Aut}(V(H, G_1))$ coincides with the so-called 2-*closure* of the permutation group $(G; H)$ (see [6]). We denote it by $G^{(2)}$ as in [6]. The mapping $G \to G^{(2)}$ satisfies the usual properties of the closure operator:

$$G_1 \subseteq G_2 \Rightarrow G_1^{(2)} \subset G_2^{(2)};$$

$$(G^{(2)})^{(2)} = G^{(2)};$$

$$G \subseteq G^{(2)}.$$

2.3. Schur rings over cyclic groups

We need some facts about Schur rings over cyclic groups.

Let C_n be the cyclic group of order n. For any divisor $m|n$ we shall denote the unique cyclic subgroup of order m by C_m. For any element $\eta = \sum_{h \in C_n} c_h h \in \mathbb{Q}C_n$ (resp. a subset $T \subseteq C_n$) and any integer m we define $\eta^{(m)} = \sum_{h \in C_n} c_h h^m$ (resp. $T^{(m)} = \{t^m \mid t \in T\}$). If m and n are relatively prime, then the element $\eta^{(m)}$ (resp. the set $T^{(m)}$) is said to be *conjugate* to η (resp. to T).

For any $T \subseteq C_n$ and p a prime dividing n we set $T^{[p]} = \{t^p \mid t \in T \text{ and } tC_p \not\subseteq T\}$.

Lemma 2.3 ([7]). *Let $\mathscr{A}$ be an S-ring over C_n and p be a prime dividing n. Then $T^{[p]} \in \mathscr{A}$ whenever $T \in \mathscr{A}$.*

Let $T \subseteq C_n$. We define the *radical* of T, $\mathrm{rad}(T)$ by the formula

$$\mathrm{rad}(T) = \{g \in C_n \mid gT = T\}.$$

It is clear that T is a union of $\mathrm{rad}(T)$-cosets. Moreover, $\mathrm{rad}(T)$ contains any subgroup $H \leqslant C_n$ such that T is a union of H-cosets. The statement below is a simple reformulation of Proposition 23.5 in [11].

Lemma 2.4. *If T is a set belonging to an S-ring $\mathscr{A}$, then* $\mathrm{rad}(T) \in \mathscr{A}$.

An S-ring $\mathscr{A} = \langle \underline{T}_0, \underline{T}_1, \ldots, \underline{T}_r \rangle$ is called *imprimitive* if there exists a proper nontrivial subgroup $F < H$ such that $\underline{F} \in \mathscr{A}$. Otherwise $\mathscr{A}$ is called *primitive.*

Let $\mathscr{A} = \langle \underline{T}_0, \underline{T}_1, \ldots, \underline{T}_r \rangle$ be an imprimitive S-ring over H that contains a normal subgroup $N \lhd H$, i.e., $\underline{N} \in \mathscr{A}$. Using this subgroup one can define a *factor* [10] S-ring $\mathscr{A}//N$ over G/N by taking the sets T_iN/N, $1 \leqslant i \leqslant r$ as basic ones.

3. Proof of the main result

3.1. The general scheme of the proof

In this subsection n is assumed to be an arbitrary natural number, not necessarily almost square-free.

Our approach to the proof of Theorem 2.1 is based on the group-theoretical reformulation of Ádám's conjecture first given in [2] and [12]. We say that a permutation group $G \leqslant S(C_n)$[2] is an *Ádám group* if any two regular cyclic subgroups of G are conjugate in G. The statement below may be found in [2].

Theorem 3.1. *Ádám's conjecture is true for a given number n if and only if the automorphism group of each n-vertex circulant graph is an Ádám group.*

Using this result and the fact that an automorphism group of any graph is 2-closed one can derive Theorem 2.1 from the following claim.

Theorem 3.2. *Any 2-closed permutation group $(G; C_n)$ of an almost square-free degree n is an Ádám group.*

In studying of 2-closed permutation groups with a regular cyclic subgroup the following notion seems to be useful. Let $(G; C_n)$ be a 2-closed permutation group that contains a regular cyclic subgroup. We say that $(G; C_n)$ is *critical* if every 2-closed permutation group $(H; C_m)$ is an Ádám group whenever $|H| \mid |G|, m \mid n$ and $(|H|, m) \neq (|G|, n)$.

The motivation for this notion is given in the following claim.

Proposition 3.3. *Theorem* 3.2 *is true if every critical permutation group of an almost square-free degree is an Ádám group.*

[2] Here and later on $S(A)$ denotes the symmetric group defined on the set A.

Proof. Assume that Theorem 3.2 is not true and take $(G; C_n)$ to be a counterexample with a minimal value of $|G|n$. To get a contradiction it is enough to show that $(G; C_n)$ is critical. Consider an arbitrary permutation group $(H; C_m)$ where H is 2-closed, contains a regular cyclic subgroup C_m and satisfies the following conditions $|H| \mid |G|, m \mid n, (|G|, n) \neq (|H|, m)$. Since $m|n$, H is also of an almost square-free degree. Combining the conditions $|H| \mid |G|, m \mid n$ with $(|G|, n) \neq (|H|, m)$ we obtain that $|H|m < |G|n$. By minimality of $(G; C_n)$ we have that $(H; C_m)$ is an Ádám group. Therefore, $(G; C_n)$ is critical. A contradiction. □

This Proposition shows that Theorem 3.2 is a consequence of the following claim.

Theorem 3.4. *Each critical permutation group of an almost square-free degree is an Ádám group.*

If critical permutation group is primitive, then the above theorem is a consequence of the following statement.

Lemma 3.5 ([7]). *Every primitive 2-closed permutation group $(G; C_n)$ is an Ádám group.*

Thus we may assume that $(G; C_n)$ is an imprimitive critical permutation group. Let δ be an arbitrary G-invariant nontrivial imprimitivity system with k blocks $\Delta_1, \ldots, \Delta_k$ (we write this as $\delta = \{\Delta_1, \ldots, \Delta_k\}$). We set $G_\delta := \{g \in G \mid \Delta_i^g = \Delta_i,\ i = 1, \ldots, k\}$ and $G^\delta = G/G_\delta$. An induced permutation group $(G^\delta; \delta)$ contains a regular cyclic subgroup C_k of order k. As usual, δ is said to be *maximal* if $(G^\delta; \delta)$ is a primitive permutation group. The statements below are slight reformulations of Theorem 3.3 and Proposition 3.2 in [7].

Proposition 3.6 ([7]). *Let $(G; C_n)$ be a permutation group of an arbitrary degree n. If both $(G^\delta; \delta)$ and $(G_\delta C_n; C_n)$ are Ádám groups, then $(G; C_n)$ is an Ádám group as well.*

Proposition 3.7 ([7]). *Let $(G; C_n)$ be a 2-closed permutation group of an arbitrary degree n. Let δ be an imprimitivity system of G. Then $(G_\delta C_n; C_n)$ is 2-closed.*

Since $|G_\delta C_n| < |G|$ is equivalent to $|\delta| < |G^\delta|$, we may formulate the following statement.

Lemma 3.8. *Let $(G; C_n)$ be a critical permutation group of an arbitrary degree n. If $|\delta| < |G^\delta|$ and $(G^\delta; \delta)$ is an Ádám group, then $(G; C_n)$ is an Ádám group as well.*

Proof. Since $|\delta| < |G^\delta|$, $|G_\delta C_n| \mid |G|$ and $|G_\delta C_n| < |G|$. Furthermore, G is critical and $(G_\delta C_n; C_n)$ is 2-closed, therefore, $(G_\delta C_n; C_n)$ is an Ádám group. Now Proposition 3.6 finishes the proof. □

If $|\delta|$ is a prime number, then (G^δ, δ) is an Ádám group due to Sylow's theorems. Therefore, by Lemma 3.8 a critical permutation group $(G; C_n)$ is an Ádám group whenever $|\delta| < |G^\delta|$. In the case of $|\delta| = |G^\delta|$ we have the following

Lemma 3.9 ([7]). *Let $(G; C_n)$ be an imprimitive critical permutation group of a square-free degree n. Let δ be a G-invariant imprimitivity system with minimal value of $|\delta|$. Assume that $G_\delta C_n = G$ and $|\delta|$ is a prime. Then G is an Ádám group.*

Fortunately, the assumptions of this claim may be weakened without any change of its proof. More precisely, the same arguments as in [7] yield us the following

Lemma 3.10. *Let $(G; C_n)$ be an imprimitive critical permutation group of an arbitrary degree n. Let δ be a maximal G-invariant imprimitivity system. Assume that $G_\delta C_n = G$, $|\delta|$ is a prime and* $\gcd(|\delta|, n/|\delta|) = 1$. *Then G is an Ádám group.*

Remark. Maximality of δ and the equality $G_\delta C_n = G$ imply that $|\delta|$ is a prime, and, therefore, this condition may be omitted.

In the case when $|\delta|$ is a composite number we have the following

Lemma 3.11 ([7]). *Let $(G; C_n)$ be an imprimitive critical permutation group of a square-free degree n. Let δ be a G-invariant imprimitivity system with minimal value of $|\delta|$. Assume that $|\delta|$ is a composite number. Then $G^\delta = S(\delta)$.*

As before, this statement may be generalized without changing of its proof.

Lemma 3.12. *Let $(G; C_n)$ be an imprimitive critical permutation group of an arbitrary degree n. Let δ be a G-invariant maximal imprimitivity system. Assume that $|\delta|$ is a composite number and* $\gcd(|\delta|, n/|\delta|) = 1$. *Then $G^\delta = S(\delta)$.*

Combining Lemmas 3.8, 3.12 and 3.10 we obtain

Theorem 3.13. *Let $(G; C_n)$ be an imprimitive critical permutation group of an arbitrary degree n. Let δ be a G-invariant maximal imprimitivity system. If* $\gcd(|\delta|, n/|\delta|) = 1$, *then $(G; C_n)$ is an Ádám group.*

3.2. Wreath product and some of its subgroups

Let us recall the notion of a *wreath* product [5]. In contrast to [5], we use Kalužnin's notation for the wreath product, where the two factors are interchanged.

Let $(A;X)$ and $(B;Y)$ be two permutation groups. Their *wreath product* $(A;X)\wr(B;Y)$ is the permutation group consisting of *tables* $[a,\alpha]$, $a\in A$, $\alpha: X\to B$. The action of $[a,\alpha]$ on the set $X\times Y$ is defined by the formula $(x,y)^{[a,\alpha]}=(x^a, y^{\alpha(x)})$.

Through this subsection we assume that $(G;C_n)\geqslant(C_n;C_n)$ is a 2-closed permutation group which has a unique maximal imprimitivity system with k blocks. Denote $m:=n/k$ just for a brevity. Since there is a bijection between subgroups of C_n belonging to $V(C_n,G_1)$ and G-invariant imprimitivity systems, an S-ring $V(C_n,G_1)$ has the following fundamental property. For each $l|n$, $l\neq n$ an inclusion $\underline{C}_l\in V(C_n,G_1)$ implies $C_l\subseteq C_m$. In other words, the set of all proper C_n-subgroups belonging to $V(C_n,G_1)$ contains a unique maximal element: C_m.

Theorem 3.14. *Let n be an almost square free number. Let $\mathscr{A}$ be a Schur ring over C_n such that C_m, $m|n$, $m\neq n$ is a unique maximal subgroup among all proper subgroups belonging to $\mathscr{A}$. Then either*

(i) *For each basic set $T\in\mathscr{A}$ it holds that $T\not\subseteq C_m \Rightarrow TC_m=T$*

or

(ii) *$n=4k$, $m=2k$, $\underline{C}_k\in\mathscr{A}$, and $C_n\setminus C_m$ is a union of two basic sets: gC_k and g^3C_k, where g is a generator of $C_4\leqslant C_{4k}$.*

Proof. Assume that there is a basic set $T\in\mathscr{A}$ such that $T\not\subseteq C_m$ and $C_m\not\subseteq \mathrm{rad}(T)$. We set $C_k:=\mathrm{rad}(T)$.

Since $\mathrm{rad}(T)\in\mathscr{A}$ and $\mathrm{rad}(T)\neq C_n$, it holds that $C_k\in\mathscr{A}$ and $C_k\neq C_n$. Consider a factor S-ring $\overline{\mathscr{A}}=\mathscr{A}//\mathrm{rad}(T)$ over $C_n/C_k=C_{n/k}$. It follows from the assumption that $C_k\subseteq C_m$. Together with $C_m\not\subseteq C_k$ this implies that $C_{m/k}$ is a nontrivial and proper subgroup of $C_{n/k}$. It contains all proper subgroups of $C_{n/k}$ belonging to $\overline{\mathscr{A}}$. $\overline{\mathscr{A}}$ is imprimitive, since $C_{m/k}\in\overline{\mathscr{A}}$.

$\overline{T}=TC_k/C_k$ is a basic set of $\overline{\mathscr{A}}$. Moreover, $\overline{T}$ has a trivial radical. Further, $T\not\subseteq C_m$ and $TC_k=T$ implies $\overline{T}\not\subseteq C_{m/k}$. Taking into account that $\langle\overline{T}\rangle\in\overline{\mathscr{A}}$ we obtain $\langle\overline{T}\rangle=C_{n/k}$.

According to Theorem 3.1 of [8] $\overline{T}=\overline{R}C_{d_1}^{\#}\cdots C_{d_r}^{\#}$ where $\overline{R}$ is an orbit of some subgroup of $\mathrm{Aut}(C_{n/k})$, $C_{d_i}\in\overline{\mathscr{A}}$ and the numbers $d_0=\mathrm{o}(\overline{R}),d_1,\ldots,d_r$ are relatively prime (here $C_d^{\#}=C_d\setminus\{\overline{1}\}$ and $\mathrm{o}(\overline{R})$ is an order of $r\in\overline{R}$). Clearly, $C_{d_0}=\langle\overline{R}\rangle$ and $C_{d_0}\in\overline{\mathscr{A}}$.

Case A: $\overline{R}=\{\overline{1}\}$. Since $C_{d_i}^{\#}\neq\emptyset$, $d_i\geqslant 2$ for all $i\geqslant 1$. If $r=1$, then $\overline{T}=C_{d_1}^{\#}$. On the other hand, $\langle\overline{T}\rangle=C_{n/k}$ implying $d_1=n/k$. Therefore $C_{n/k}^{\#}$ is a basic set of $\overline{\mathscr{A}}$, i.e., $\overline{\mathscr{A}}$ is trivial contrary to being imprimitive.

If $r\geqslant 2$, then $\gcd(d_i,d_j)=1$ whenever $i\neq j$. Hence each C_{d_i}, $i=1,\ldots,r$ is a proper subgroup of $C_{n/k}$. Therefore $C_{d_i}\subseteq C_{m/k}$ for each $i=1,\ldots,r$. This implies $\overline{T}\subset C_{m/k}$ contrary to $\langle\overline{T}\rangle=C_{n/k}$.

Thus this case is impossible.

Case B: $\overline{R} \neq \{\overline{1}\} \Leftrightarrow d_0 > 1$. If $r \geqslant 1$, then for each $1 \leqslant i \leqslant r$ it holds that $\gcd(d_0, d_i) = 1$ implying that $C_{d_0}, C_{d_1}, \ldots, C_{d_r}$ are proper subgroups of $C_{n/k}$. Since $C_{d_i} \in \overline{\mathscr{A}}$, $C_{d_i} \subseteq C_{m/k}$ for all $i = 0, \ldots, r$. Therefore $\overline{T} \subseteq C_{m/k}$ contrary to $\langle \overline{T} \rangle = C_{n/k}$.

Thus we may assume that $r = 0$, i.e., $\overline{T} = \overline{R}$. All elements of $\overline{T}$ are of the same order d_0. Therefore $|\langle \overline{T} \rangle| = d_0$. Since $\langle \overline{T} \rangle = C_{n/k}$, $d_0 = n/k$.

$\overline{\mathscr{A}}$ is an imprimitive S-ring over $C_{n/k}$, hence n/k has at least two prime divisors, say p and q.

Assume first that $p \neq q$. Since $\mathrm{rad}(\overline{T})$ is trivial, both $\overline{T}^{[p]}$ and $\overline{T}^{[q]}$ are not empty. But subgroups $\langle \overline{T}^{[p]} \rangle = C_{n/kp}$ and $\langle \overline{T}^{[q]} \rangle = C_{n/kq}$ are two distinct maximal subgroups belonging to $\overline{\mathscr{A}}$. A contradiciton. Therefore $p = q$, which, in turn, implies $p = q = 2, d_0 = 4$, $n = 4k$, $m = 2k$. Furthermore, $C_2 \in \overline{\mathscr{A}}$, $\langle \overline{T} \rangle = C_4$ and $\mathrm{rad}(\overline{T}) = \{\overline{1}\}$. Therefore, either $\overline{T} = \{gC_k\}$ or $\overline{T} = \{g^{-1}C_k\}$. Now the claim is evident. □

If transitivity module $V(C_n, G_1)$has the structure corresponding to the part (i) of the above claim, then its automorphism group is a wreath product of permutation groups. In order to formulate the corresponding claim we need an additional notation. We set $\mathscr{A}_m := \mathscr{A} \cap ZC_m$. If $C_m \in \mathscr{A}$, then $\mathscr{A}_m$ is an S-ring over C_m whose basic sets are those of $\mathscr{A}$ contained in C_m.

Theorem 3.15. *Let $\mathscr{A}$ be a Schur ring over C_n. Assume that there exists $m|n$ such that $\underline{C}_m \in \mathscr{A}$ and for each basic set $T \in \mathscr{A}$ the following condition is satisfied*:

$$T \not\subseteq C_m \Rightarrow TC_m = T.$$

Then $\mathrm{Aut}(\mathscr{A})$ *is isomorphic as permutation group to* $\mathrm{Aut}(\mathscr{A}//C_m) \wr \mathrm{Aut}(\mathscr{A}_m)$.

Proof. Take an arbitrary $\pi \in \mathrm{Aut}(\mathscr{A})$. Since $\underline{C}_m \in \mathscr{A}$, the cosets gC_m, $g \in C_n$ are blocks of an imprimitivity system which is invariant under the action of $\mathrm{Aut}(\mathscr{A})$. Let $g \in C_n$ be a generator of C_n. Then $1, g, \ldots, g^{n/m-1}$ is a complete set of representatives of C_m-cosets. Denote by $a \in S_{n/m}$ a permutation of C_m-cosets induced by π, i.e., $(g^iC_m)^\pi = g^{i^a}C_m$. Thus π may be written as a pair $[a, \alpha(x)]$, $a \in S_{n/m}, \alpha : \{0, 1, \ldots, n/m-1\} \to S_m$ whose action on C_n is defined by the following rule:

$$(g^ih)^{[a,\alpha(x)]} = g^{i^a}h^{\alpha(i)}, \quad 0 \leqslant i < n/m, \ h \in C_m.$$

We have to show that $a \in \mathrm{Aut}(\mathscr{A}//C_m)$ and $\alpha(i) \in \mathrm{Aut}(\mathscr{A}_m)$ for each $0 \leqslant i < n/m$.

Consider an arbitrary basic set T of $\mathscr{A}$. Take a pair $(g^iC_m, g^jC_m) \in C_n/C_m \times C_n/C_m$ satisfying $g^iC_m(g^jC_m)^{-1} \in TC_m/C_m$. Then $(g^{i^a}C_m)\ (g^{j^a}C_m)^{-1} = (g^iC_m)^\pi\ ((g^jC_m)^\pi)^{-1} = (g^i)^\pi C_m((g^j)^\pi)^{-1}C_m$. Since π is an automorphism of $\mathscr{A}$ and $g^i(g^j)^{-1} \in T$, $(g^i)^\pi((g^j)^\pi)^{-1} \in T$, whence $(g^i)^\pi C_m((g^j)^\pi)^{-1}C_m \in TC_m/C_m$. Thus $a \in \mathrm{Aut}(\mathscr{A}//C_m)$.

Take now a basic set $T \subseteq C_m$ and a pair (g^ih_1, g^ih_2) such that $h_1h_2^{-1} \in T$. Since $\pi = [a, \alpha(x)]$ is an automorphism of $\mathscr{A}$, the inclusion $(g^ih_1)^\pi((g^ih_2)^\pi)^{-1} \in T$ should hold. Taking into account that

$$(g^i h_j)^{[a,\alpha(x)]} = g^{i^a} h_j^{\alpha(i)}, \quad j = 1,2,$$

we obtain $h_1^{\alpha(i)}(h_2^{\alpha(i)})^{-1} \in T$. Therefore $\alpha(i) \in \mathrm{Aut}(\mathcal{A}_m)$ for every $i = 0,\dots,n/m-1$.

Thus we have shown that $[a,\alpha(x)] \in \mathrm{Aut}(\mathcal{A}//C_m) \wr \mathrm{Aut}(\mathcal{A}_m)$.

To prove our statement in opposite direction, consider an arbitrary pair $\pi = [a,\alpha(x)]$, where $a \in \mathrm{Aut}(\mathcal{A}//C_m)$ and $\alpha : \{0,\dots,n/m-1\} \to \mathrm{Aut}(\mathcal{A}_m)$. We have to show that for each basic set $T \in \mathcal{A}$ the following holds:

$$xy^{-1} \in T \Rightarrow x^\pi (y^\pi)^{-1} \in T.$$

Consider at first the case of $T \subseteq C_m$. Each pair (x,y) with $xy^{-1} \in T$ may be written as $x = g^i h_1$, $y = g^i h_2$ for suitable i and $h_1, h_2 \in C_m$. Clearly $h_1 h_2^{-1} \in T$. According to a definition of a and $\alpha(x)$, $x^\pi = g^{i^a} h_1^{\alpha(i)}$, $y^\pi = g^{i^a} h_2^{\alpha(i)}$. Since $\alpha(i)$ is an automorphism of $\mathcal{A}_m$, $h_1^{\alpha(i)}(h_2^{\alpha(i)})^{-1} \in T$, which, in turn, implies the required inclusion $x^\pi (y^\pi)^{-1} \in T$.

Let now $T \not\subseteq C_m$. Then $C_m T = T$, according to our assumption. As before, let $xy^{-1} \in T$. Writing x and y as $x = g^i h_1$, $y = g^j h_2$, $i \neq j$, $h_1, h_2 \in C_m$ and applying $\pi = [a,\alpha(x)]$ to both of them we obtain:

$$x^\pi = g^{i^a} h_1^{\alpha(i)}, \qquad y^\pi = g^{j^a} h_2^{\alpha(j)}. \tag{$*$}$$

Since $a \in \mathrm{Aut}(\mathcal{A}//C_m)$ and $g^i C_m (g^j C_m)^{-1} \in TC_m/C_m$, $g^{i^a} C_m (g^{j^a} C_m)^{-1} \in TC_m/C_m$, or, equivalently, $g^{i^a}(g^{j^a})^{-1} \in TC_m = T$. Combining this with $(*)$ we obtain

$$x^\pi (y^\pi)^{-1} = g^{i^a}(g^{j^a})^{-1} h_1^{\alpha(i)} (h_2^{\alpha(j)})^{-1} \in g^{i^a}(g^{j^a})^{-1} C_m \subseteq TC_m = T,$$

as required. □

If the structure of $V(C_n, G_1)$looks as in Theorem 3.14(ii), then its automorphism group has more complicated structure. To describe this structure consider a group $\mathrm{Aut}(\mathcal{A}_{2k})$. Since $C_k \in \mathcal{A}$, the partition $C_k \cup (C_{2k} \setminus C_k)$ is an imprimitivity system of $\mathrm{Aut}(\mathcal{A}_{2k})$. Thus we can define a homomorphism $\varepsilon : \mathrm{Aut}(\mathcal{A}_{2k}) \to S(\{0,1\})$:

$$\varepsilon(\pi) = \begin{cases} \mathrm{id} & \text{if } C_k^\pi = C_k, \\ (0,1) & \text{if } C_k^\pi = C_k g^2. \end{cases} \tag{$**$}$$

Proposition 3.16. *Let $\mathcal{A}$ be an S-ring over C_{4k} (k is odd and square-free) which satisfies the following conditions:*

(i) $C_k, C_{2k} \in \mathcal{A}$;

(ii) *$gC_k, g^3 C_k$ are basic sets of $\mathcal{A}$, where g is a generator of order 4.*

Then

$$\mathrm{Aut}(\mathcal{A}) = \{[a,\alpha(x)] \mid a \in S(\{0,1\}),\ \alpha : \{0,1\} \to \mathrm{Aut}(\mathcal{A}_{2k}),\ a = \varepsilon(\alpha(0)\alpha(1))\},$$

where ε is a homomorphism defined above. The action of $\mathrm{Aut}(\mathcal{A})$ *on C_{4k} is defined as follows*:

$$(g^i h)^{[a,\alpha(x)]} = g^{i^a} h^{\alpha(i)}, \quad i = 0,1,\ h \in C_{2k}.$$

Proof. As a $\boldsymbol{Z}$-module $\mathscr{A}=\mathscr{A}'+\boldsymbol{Z}\underline{gC_k}$, where $\mathscr{A}'=\mathscr{A}_{2k}+\boldsymbol{Z}\underline{gC_{2k}}$. Therefore $\mathrm{Aut}(\mathscr{A}) = \mathrm{Aut}(\mathscr{A}')\cap \mathrm{Aut}(\Gamma_{4k}(gC_k))$. According to Theorem 3.15 $\mathrm{Aut}(\mathscr{A}')=S(\{0,1\})\wr \mathrm{Aut}(\mathscr{A}_{2k})$ and its action on C_{4k} is defined by the following formula:

$$(g^ih)^{[a,\alpha(x)]}=g^{i^a}h^{\alpha(i)},\quad i=0,1,\quad h\in C_{2k}.$$

Thus we have only to show that $[a,\alpha(x)]\in \mathrm{Aut}(\Gamma_{4k}(gC_k))$ if and only if $a=\varepsilon(\alpha(0)\alpha(1))$.

Assume first that $a=\varepsilon(\alpha(0)\alpha(1))$ and show that $[a,\alpha]\in \mathrm{Aut}(\mathscr{A})$.

Take a pair $x=g^ih_1,\ y=g^jh_2,\ h_i\in C_{2k},\ i,j\in\{0,1\}$ with $xy^{-1}\in gC_k$. Since $gC_k\cap C_{2k}=\emptyset$, $i\neq j$. Therefore either

$$i=1,\quad j=0,\quad h_1h_2^{-1}\in C_k,$$

or

$$i=0,\quad j=1,\quad h_1h_2^{-1}\in C_kg^2.$$

Applying π we obtain

$$x^\pi=g^{i^a}h_1^{\alpha(i)};\qquad y^\pi=g^{j^a}h_2^{\alpha(j)}$$

and

$$x^\pi(y^\pi)^{-1}=g^{i^a}(g^{j^a})^{-1}h_1^{\alpha(i)}(h_2^{\alpha(j)})^{-1}.$$

If $a=id$, then $i^a=i,\ j^a=j$ and $\varepsilon(\alpha(0))=\varepsilon(\alpha(1))$ implying $h_2^{\alpha(j)}\equiv h_2^{\alpha(i)}\ (\mathrm{mod}\ C_k)$, Therefore

$$x^\pi(y^\pi)^{-1}\equiv g^i(g^j)^{-1}h_1^{\alpha(i)}(h_2^{\alpha(i)})^{-1}\ (\mathrm{mod}\ C_k).$$

Since $\alpha(0),\alpha(1)\in \mathrm{Aut}(\mathscr{A}_{2k})$ and $\underline{C_k}\in\mathscr{A}_{2k}$,

$$h_1^{\alpha(i)}(h_2^{\alpha(i)})^{-1}\equiv h_1h_2^{-1}\ (\mathrm{mod}\ C_k).$$

Therefore

$$x^\pi(y^\pi)^{-1}\equiv xy^{-1}\ (\mathrm{mod}\ C_k),$$

implying $x^\pi(y^\pi)^{-1}\in xy^{-1}C_k=gC_k$ as required.

If $a=(0,1)$, then $i^a=j,\ j^a=i$ and $\varepsilon(\alpha(0))=(0,1)\varepsilon(\alpha(1))$ implying $h_2^{\alpha(i)}\equiv h_2^{\alpha(j)}g^2\ (\mathrm{mod}\ C_k)$. Thus we can write the following sequence of congruences:

$$\begin{aligned}x^\pi(y^\pi)^{-1}&\equiv g^j(g^i)^{-1}h_1^{\alpha(i)}g^{-2}(h_2^{\alpha(i)})^{-1}\equiv g^{-2}g^j(g^i)^{-1}h_1h_2^{-1}\\&\equiv g^i(g^j)^{-1}h_1h_2^{-1}\equiv xy^{-1}\ (\mathrm{mod}\ C_k);\end{aligned}$$

that proves $[a,\alpha]\in \mathrm{Aut}(\mathscr{A})$.

Thus $\mathrm{Aut}(\mathscr{A})$ contains all tables $[a,\alpha]$ that satisfy $a=\varepsilon(\alpha(0)\alpha(1))$. The subset of all such tables is a subgroup of $S(\{0,1\})\wr \mathrm{Aut}(\mathscr{A}_{2k})$ of index 2. On the other hand, $\mathrm{Aut}(\mathscr{A})\neq S(\{0,1\})\wr \mathrm{Aut}(\mathscr{A}_{2k})$, since $C_{4k}\setminus C_{2k}$ is not a basic set of $\mathscr{A}$. Hence

$$\mathrm{Aut}(\mathscr{A})=\{[a,\alpha(x)]\mid a\in S(\{0,1\}),\ \alpha:\{0,1\}\to \mathrm{Aut}(\mathscr{A}_{2k}),\ a=\varepsilon(\alpha(0)\alpha(1))\},$$

as desired. □

Our next step is to describe the conjugacy classes of regular cycles in a wreath product of permutation groups.[3]

Lemma 3.17. *Let $(G;X), |X|=n$ and $(H;Y), |Y|=m$ be two permutation groups.*

(i) *An element $[a,\alpha]\in(G;X)\wr(H;Y)$ is a regular cycle if and only if both a and $\alpha(x)\alpha(x^a)\cdot\ldots\cdot\alpha(x^{a^{n-1}})$ are regular cycles in the corresponding permutation groups.*

(ii) *Two regular cycles $[a,\alpha],[b,\beta]\in(G;X)\wr(H;Y)$ are conjugate in $(G;X)\wr(H;Y)$ if and only if a,b are conjugate in G, and $\alpha(x)\alpha(x^a)\cdot\ldots\cdot\alpha(x^{a^{n-1}})$, $\beta(x)\beta(x^b)\cdot\ldots\cdot\beta(x^{b^{n-1}})$ are conjugate in $(H;Y)$.*

Proof. (i) The proof of this part is easy, so we omit it.

(ii) Let $[a,\alpha(x)]$ and $[b,\beta(x)]$ be two regular cycles that are conjugate in $(G;X)\wr(H;Y)$ by $[c,\gamma(x)]$. That means

$$[a,\alpha(x)][c,\gamma(x)]=[c,\gamma(x)][b,\beta(x)],$$

or, equivalently, $a^c=b$ and $\alpha(x)\gamma(x^a)=\gamma(x)\beta(x^c)$ for all $x\in X$. Since a is a regular cycle on X, the latter equality may be rewritten as follows:

$$\begin{aligned}
&\gamma^{-1}(x)\alpha(x)\gamma(x^a)=\beta(x^c),\\
&\gamma^{-1}(x^a)\alpha(x^a)\gamma(x^{a^2})=\beta(x^{ac}),\\
&\vdots\\
&\gamma^{-1}(x^{a^{i-1}})\alpha(x^{a^{i-1}})\gamma(x^{a^i})=\beta(x^{a^ic}),\\
&\vdots\\
&\gamma^{-1}(x^{a^{n-1}})\alpha(x^{a^{n-1}})\gamma(x^{a^n})=\beta(x^{a^{n-1}c}).
\end{aligned}\qquad (***)$$

Multiplying all these equalities and taking into account that $a^n=1$ gives us

$$\begin{aligned}
\gamma^{-1}(x)\alpha(x)\alpha(x^a)\cdot\ldots\cdot\alpha(x^{a^{n-1}})\gamma(x)&=\beta(x^c)\beta(x^{ac})\cdot\ldots\cdot\beta(x^{a^{n-1}c})\\
&=\beta(x')\beta(x'^b)\cdot\ldots\cdot\beta(x'^{b^{n-1}}),
\end{aligned}$$

where $x'=x^c$. Thus $\alpha(x)\alpha(x^a)\cdot\ldots\cdot\alpha(x^{a^{n-1}})$ is conjugate to $\beta(x')\beta(x'^b)\cdot\ldots\cdot\beta(x'^{b^{n-1}})$ and, therefore, conjugate to $\beta(x)\beta(x^b)\cdot\ldots\cdot\beta(x^{b^{n-1}})$.

Assume now that $a,b\in G$ are two regular cycles conjugate in $(G;X)$ and $\alpha(x)\alpha(x^a)\cdot\ldots\cdot\alpha(x^{a^{n-1}}),\beta(x)\beta(x^b)\cdot\ldots\cdot\beta(x^{b^{n-1}})$ are two regular cycles conjugate in $(H;Y)$. Therefore $a^c=b$ for a suitable $c\in G$. Since $\beta(x)\beta(x^b)\cdot\ldots\cdot\beta(x^{b^{n-1}})$ is conjugate to $\beta(x')\beta(x'^b)\cdot\ldots\cdot\beta(x'^{b^{n-1}})$ for every $x'\in X$, there exists $\pi\in(H;Y)$ such that $\pi^{-1}\alpha(x)\alpha(x^a)\cdot\ldots\cdot\alpha(x^{a^{n-1}})\pi=\beta(x^c)\beta(x^{cb})\cdot\ldots\cdot\beta(x^{cb^{n-1}})$. Define $\gamma: X\to H$ as follows: $\gamma(x)=\pi$ and $\gamma(x^{a^i})=\alpha^{-1}(x^{a^{i-1}})\gamma(x^{a^{i-1}})\beta(x^{a^{i-1}c})$ for all $1\leqslant i\leqslant n-1$. Since $\pi^{-1}\alpha(x)\alpha(x^a)\cdot\ldots\cdot\alpha(x^{a^{n-1}})\pi=\beta(x^c)\beta(x^{cb})\cdot\ldots\cdot\beta(x^{cb^{n-1}})$, $\gamma(x)=\alpha^{-1}(x^{a^{n-1}})\times\gamma(x^{a^{n-1}})\beta(x^{a^{n-1}c})$ and according to $(***)$, $[a,\alpha(x)]$ and $[b,\beta(x)]$ are conjugate by $[c,\gamma(x)]$. □

[3] Here, a regular cycle means a cyclic permutation without fixed points.

We need the following lemma.

Lemma 3.18. *Let* $[a,\alpha(x)],[b,\beta(x)]\in(G;X)\wr(H;Y)$, $|X|=n$, $|Y|=m$ *be two regular cycles such that*

(i) a^k *is conjugate to* b *for a suitable* $k, \gcd(k,n)=1$;

(ii) $(\alpha(x)\alpha(x^a)\cdot\ldots\cdot\alpha(x^{a^{n-1}}))^l$ *is conjugate to* $\beta(x)\beta(x^b)\cdot\ldots\cdot\beta(x^{b^{n-1}})$ *for an appropriate* $l, \gcd(l,m)=1$.

If there exists a $q\in\mathbf{Z}$ *with* $q\equiv l\,(\operatorname{mod} m)$ *and* $q\equiv k\,(\operatorname{mod} n)$, *then* $[a,\alpha(x)]^q$ *is conjugate to* $[b,\beta(x)]$ *in the group* $(G;X)\wr(H;Y)$.

Proof. Set $[c,\gamma(x)] := [a,\alpha(x)]^q$. Clearly $c=a^q=a^k$ is a regular cycle due to (i). Furthermore,

$$\begin{aligned}
&\gamma(x)\gamma(x^c)\cdot\ldots\cdot\gamma(x^{c^{n-1}})\\
&\quad=\gamma(x)\gamma(x^{a^q})\cdot\ldots\cdot\gamma(x^{a^{qn-q}})\\
&\quad=\alpha(x)\alpha(x^a)\cdot\ldots\cdot\alpha(x^{a^{q-1}})\cdot\alpha(x^{a^q})\alpha(x^{a^{q+1}})\cdot\ldots\cdot\alpha(x^{a^{2q-1}})\cdot\ldots\cdot\\
&\qquad\alpha(x^{a^{qn-q}})\alpha(x^{a^{qn-q+1}})\cdot\ldots\cdot\alpha(x^{a^{nq-1}})\\
&\quad=\prod_{i=0}^{qn-1}\alpha(x^{a^i}).
\end{aligned}$$

Since $a^n=1$, the latter expression may be written as follows:

$$\prod_{i=0}^{qn-1}\alpha(x^{a^i})=(\alpha(x)\alpha(x^a)\cdot\ldots\cdot\alpha(x^{a^{n-1}}))^q=(\alpha(x)\alpha(x^a)\cdot\ldots\cdot\alpha(x^{a^{n-1}}))^l.$$

Thus c is conjugate to b in G and $\gamma(x)\gamma(x^c)\cdot\ldots\cdot\gamma(x^{c^{n-1}})$ is conjugate to $\beta(x)\beta(x^b)\cdot\ldots\cdot\beta(x^{b^{n-1}})$.

By previous claim $[c,\gamma(x)]$ and $[b,\beta(x)]$ are conjugate in $(G;X)\wr(H;Y)$. □

3.3. Proof of Theorem 3.4

Let $(G;C_n)$ be a critical, and, therefore, 2-closed permutation group of an almost square-free degree n. According to Lemma 3.5 we may assume that $(G;C_n)$ is an imprimitive permutation group . Let δ be an imprimitivity system of $(G;C_n)$. If $\gcd(|\delta|, n/|\delta|)=1$, then we are done by Theorem 3.13. Thus we may assume that $(G;C_n)$ has a unique maximal imprimitivity system δ with $\gcd(|\delta|,n/|\delta|)$. This implies that either $|\delta|=2$ or $n/|\delta|=2$. Due to Theorems 3.14, 3.15 and Proposition 3.16 a group G is either one of the wreath products $S_2\wr(H;Y),(H;Y)\wr S_2$ or a subgroup of $S_2\wr(H;Y)$ of index 2 that was described in Proposition 3.16. In all these cases $(H;Y)$ is a 2-closed permutation group of a degree $2k$, where k is an odd square-free number. Since $(G;C_n)$ is a critical permutation group and $(H;Y)$ is 2-closed, $(H;Y)$ is an Ádám group. It follows from Lemma 3.18 that both $S_2\wr(H;Y)$ and $(H;Y)\wr S_2$ are Ádám groups. To finish the proof we have to consider the case when $(G;C_n)$ has a form described in Proposition 3.16. In this case G is a subgroup of $S_2\wr(H;Y)$

of index 2. Let $C_n \leqslant G \geqslant C_n'$ be two regular cyclic subgroups. Since $S_2 \wr (H;Y)$ is an Ádám group, $C_n^g = C_n'$ for some $g \in S_2 \wr (H;Y)$. If $g \in G$, then we are done. If $g \notin G$, then $g = g_0 g_1$, where $g_0 = [(0,1); \mathrm{id}, \mathrm{id}]$ and $g_1 \in G$. Thus it is enough to show that $C_n^{g_0}$ and C_n are conjugate in G.

According to Proposition 3.16, $G = \{[a; \alpha(0), \alpha(1)] \mid \alpha(i) \in H$ and $\varepsilon(\alpha(0)\alpha(1)) = a\}$ where ε is a homomorphism defined by $(**)$. Let $C_n = \langle [a; \alpha(0), \alpha(1)] \rangle$ be a regular cyclic subgroup. According to Lemma 3.17, that means that $a = (0,1)$ and $\alpha(0)\alpha(1)$ is a regular cycle. Thus $C_n' = C_n^{g_0} = \langle [(0,1); \alpha(1), \alpha(0)] \rangle$.

Since $\gcd(k,2) = 1$, there exists $q \in \mathbf{Z}$ such that $q \equiv 0 \pmod{k}$, $q \equiv 1 \pmod{4}$. Then $\gcd(2q+1, 4k) = 1$. We claim that $[(0,1); \alpha(0), \alpha(1)]^{2q+1}$ and $[(0,1); \alpha(1), \alpha(0)]$ are conjugate in G. Indeed, $[(0,1); \alpha(0), \alpha(1)]^{2q+1} = [(0,1); \beta(0), \beta(1)]$, where $\beta(0) = (\alpha(0)\alpha(1))^q \alpha(0)$, $\beta(1) = (\alpha(1)\alpha(0))^q \alpha(1)$. Set $\gamma(0) = \mathrm{id}$, $\gamma(1) = \alpha^{-1}(1)\beta(1) = \alpha^{-1}(1)(\alpha(1)\alpha(0))^q \alpha(1) = (\alpha(0)\alpha(1))^q$. Then

$$
\begin{aligned}
[(0,1); \alpha(1), \alpha(0)][(0,1); \gamma(0), \gamma(1)] &= [\mathrm{id}; \alpha(1)\gamma(1), \alpha(0)\gamma(0)] \\
&= [\mathrm{id}; \alpha(1)(\alpha(0)\alpha(1))^q, \alpha(0)];
\end{aligned}
$$

$$
\begin{aligned}
[(0,1); \gamma(0), \gamma(1)][(0,1); \beta(0), \beta(1)] &= [\mathrm{id}; \gamma(0)\beta(1), \gamma(1)\beta(0)] \\
&= [\mathrm{id}; (\alpha(1)\alpha(0))^q \alpha(1), (\alpha(0)\alpha(1))^{2q} \alpha(0)].
\end{aligned}
$$

Since $2q \equiv 0 \pmod{2k}$ and $\alpha(0)\alpha(1)$ is $2k$-cycle, $((\alpha(0)\alpha(1))^{2q} = \mathrm{id}$. Now it is easy to show that two above elements are equal. □

Acknowledgements

The author is very grateful to M. Klin for his attention and support of this work and for all his valuable remarks. The author would also like to thank the anonymous referee who read the paper carefully and proposed very helpful suggestions.

References

[1] A. Ádám, Research problem 2-10, J. Combin. Theory 2 (1967) 393.
[2] L. Babai, Isomorphism problem for a class of point-symmetric structures, Acta Math. Acad. Sci. Hungar. 29 (1977) 329–336.
[3] D.Ž. Djoković, Isomorphism problem for a special class of graphs, Acta Math. Acad. Sci. Hungar. 21 (1970) 267–270.
[4] B. Elspas and J. Turner, Graphs with circulant adjacency matrices, J. Combin. Theory 9 (1970) 297–307.
[5] M. Hall, Group Theory (MacMillan, New York, 1959).
[6] M.H. Klin and R. Pöschel, The König problem, the isomorphism problem for cyclic graphs and the method of Schur rings, in: Algebraic methods in graph theory, Szeged, 1978, Colloq. Math. Soc. J. Bolyai, vol. 25 (North-Holland, Amsterdam, 1981) 405–434.
[7] M. Muzychuk, Ádám's conjecture is true in the square-free case, J. Combin. Theory Ser. A 72 (1) 118–134.

[8] M. Muzychuk, On the structure of basic sets of Schur rings over cyclic groups, J. Algebra 109 (2) (1994) 655–678.
[9] P.P. Pálfy, Isomorphism problem for relational structures with a cyclic automorphism, European J. Combin. 8 (1987) 35–43.
[10] O. Tamaschke, On the theory of Schur-rings, Ann. Mat. Pura Appl. Ser. IV 81 (1969) 1–43.
[11] H. Wielandt, Finite Permutation Groups (Academic Press, Berlin, 1964).
[12] B. Alspach and T.D. Parsons, Isomorphism of circulant graphs and digraphs, Discrete Math. 25 (1979) 97–108.